MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2018/2019

ETM7106 NETWORK SECURITY

(All Sections / Groups)

31 MAY 2019
9:00 A.M – 12:00 A.M.
(3 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 7 printed pages including the cover page with 4 questions only.

2. Attempt all FOUR (4) questions. All questions carry equal marks and the distribution of marks is given in the questions.

3. Please print all your answers in the answer booklet provided.

4. State all assumptions clearly.

Question 1

(a) Your friend has developed and deployed a new encryption algorithm, but insists on keeping the cipher secret from public disclosure.

(i) What principle in cryptography is your friend violating? Elaborate briefly on the principle.

[2 marks]

(ii) What justification can you use to convince your friend that the cipher needs to be put up for public scrutiny?

[2 marks]

(b) To recover the plaintext and key, mount a ciphertext-only attack on the following ciphertext encrypted using the **Shift Cipher**:

FUUQJ

(i) What is the mathematical equation used to represent **encryption** and **decryption** in the Shift Cipher?

[2 marks]

(ii) Assuming the message and key space consists only of 26 alphabets A-Z, what is the plaintext? Write down your working to obtain the plaintext.

[2 marks]

(iii) What is the key used?

[1 mark]

(c) Answer the following questions on Advanced Encryption Standard (AES):

(i) What is the name of the cipher deployed as AES?

[1 mark]

(ii) What is the block size of AES?

[1 mark]

(iii) How many rounds does AES consist of?

[1 mark]

(iv) If the current cipher used as AES is suddenly attacked and broken, what is a recommended replacement cipher for AES?

[2 marks]

Continued...

(d) The following strings are related to AES:

Plaintext State: `00010203040506070809 0A0B0C0D0E0F`
Round Key: `00102030405060708090A0B0C0D0E0F0`

(i) Represent the **plaintext state** and **round key** as 4 × 4 matrices.

[2 marks]

(ii) Show the state from Question 1(d)(i) after initial **AddRoundKey**.

[3 marks]

(iii) Show the state from Question 1(d)(ii) after **SubBytes**, given the S-box in Figure Q1(d).

[3 marks]

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure Q1(d): S-box

(iv) Show the state from Question 1(d)(iii) after **ShiftRows**.

[3 marks]

Continued...

Question 2

(a) What is the main distinction between symmetric key cryptography and asymmetric key cryptography?

[4 marks]

(b) Suppose Alice has a secret, a and Bob has a secret, b. Using a generator g in group G of prime order p, describe in **FOUR (4)** steps how Alice and Bob can share a session key using the Diffie-Hellman key exchange protocol.

[8 marks]

(c) IP Security (IPSec) provides end-to-end security for IPv4 and IPv6.

(i) List IPSec's two main sub-protocols and their corresponding security services.

[4 marks]

(ii) Explain the IPSec's **transport-mode** and **tunnel-mode** of operation with the help of diagrams.

[4 marks]

(iii) Describe IPsec Security Associations (SAs)?

[2 marks]

(d) You are a member of a project that deals with highly confidential information.

(i) What protocol should you use to send emails securely to other team members?

[1 mark]

(ii) Describe the encryption and decryption steps to achieve confidentiality when sending an email using this protocol.

[2 marks]

Continued...

Question 3

(a) There is a term called "WarDriving" in wireless security.

(i) Describe this term.

[2 marks]

(ii) Why is it a risk to users?

[2 marks]

(iii) List **TWO (2)** methods to mitigate the risks of wardriving.

[2 marks]

(b) Describe the following attacks on wireless communications. Additionally, discuss the mitigation methods for each of these attacks.

(i) Impersonation attack [3 marks]

(ii) Interception attack [3 marks]

(iii) Fake access point [3 marks]

(c) Explain the following attacks on the Bluetooth protocol.

(i) Bluesnarfing [2 marks]

(ii) Bluejacking [2 marks]

(iii) Bluebugging [2 marks]

(d) Anonymity is defined as the state of not being identifiable. Discuss **FOUR (4)** issues that should be considered in order to maintain anonymity.

[4 marks]

Continued...

Question 4

(a) A firewall is a network security device that monitors and controls incoming and outgoing network traffic. Describe the following types of firewalls:

(i) Static firewall [2 marks]

(ii) Stateful firewall [2 marks]

(iii) Application proxy firewall [2 marks]

(b) The network topology is shown in Figure Q4(b). The network consists of two servers in the demilitarized zone (DMZ), three workstations in the internal network, and a firewall. The details are shown in Table Q4(b) below:

Table Q4(b)

Description	IP Address	Description	IP Address
Server 1 (SMTP)	1.2.3.4	Workstation 1	10.0.0.1
Server 2 (FTP)	1.2.3.5	Workstation 2	10.0.0.2
		Workstation 3	10.0.0.3

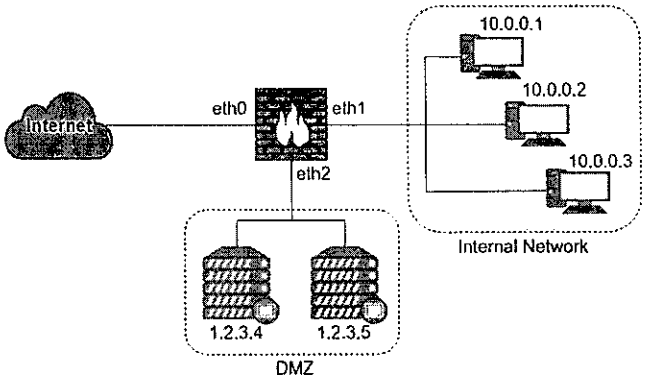

Figure Q4(b)

Continued...

- Allow all TCP connections from Internet to the SMTP server on port 25
- Allow all TCP connections from Internet to the FTP server on port 21
- Allow all outbound connections from Internal Network to Internet
- Allow all TCP connections from Internal Network to SMTP server on port 25
- Deny all connections from Internal Network to FTP server on port 21
- Deny all inbound connections from Internet to DMZ (default rule)
- Deny all inbound connections from Internet to Internal Network (default rule)

Using the security policy shown above, write the firewall ruleset using the syntax shown below:

<allow/deny> <protocol> <src ip address>:<src port> /<inbound interface> → <dest ip address>:<dest port> /<outbound interface>

Example: **allow tcp *:* /eth0 → 2.2.2.2:80 /eth2**

[7 marks]

(c) An Intrusion Detection System (IDS) is designed to detect unauthorised access to computing resources.

(i) Explain the **host-based IDS.**

[2 marks]

(ii) Explain the **network-based IDS.**

[2 marks]

(iii) What are **false positive** and **false negative** detection?

[2 marks]

(iv) How does an **anomaly-based IDS** function and what are its advantages and disadvantages?

[3 marks]

(v) How does **misuse or signature-based IDS** function and what are its advantages and disadvantages?

[3 marks]

End